TAMPEREEN AMMATTIKORKEAKOULU
Sähkötekniikan koulutusohjelma
Automaatiotekniikka

Tutkintotyö

Kristian Paakkunainen

TUOTANNONOHJAUSJÄRJESTELMIEN ETÄHALLINTA INTERNETIN VÄLITYKSELLÄ

Työn valvoja DI Mikko Numminen
Työn teettäjä Indel Automation Oy
Tampere 2005

TAMPEREEN AMMATTIKORKEAKOULU
Sähkötekniikan koulutusohjelma
Automaatiotekniikka
Paakkunainen, Kristian

Tuotannonohjausjärjestelmien etähallinta Internetin välityksellä
Tutkintotyö
37 sivua + 1 liitesivu
Työn valvoja
DI Mikko Numminen
Työn teettäjä
Indel Automation Oy, ohjaajana Pasi Mattila
Huhtikuu 2005
Hakusanat
etähallinta, etäkäyttö, etätyö, virtuaalinen yksityisverkko, VPN

TIIVISTELMÄ

Työ käsittelee tuotannonohjausjärjestelmien ylläpidollista etähallintaa Internetin välityksellä. Tuotannonohjausjärjestelmien ylläpidosta aiheutuu aina turhia matkakustannuksia, kun joudutaan menemään itse paikalle kohteeseen suorittamaan ylläpidolliset toimenpiteet. Tämän vuoksi on kehitetty etäkäyttöratkaisu, jotta ylläpidon voi suorittaa etänä Internetin välityksellä.

Työn tarkoituksena on ollut kehittää tuotannonohjausjärjestelmien ylläpitoa varten etäkäyttöratkaisu unohtamatta tietoturvaa. Suunniteltu etäkäyttöratkaisu on toteutettu käyttäen VPN-tekniikkaa, etähallintaohjelmaa ja Siemens S7 Simatic Manager -logiikkaohjelmointiohjelmaa. Etäkäyttöratkaisun suunnittelussa on keskitytty erityisesti tietoturvaan ja etähallintaohjelman valintaan.

Suunniteltu etäkäyttöratkaisu on tarkoitettu pienten yritysten edulliseksi etäkäyttöratkaisuksi ja sitä voidaan käyttää mallina suunniteltaessa uusia etäkäyttöratkaisuja. Tulevaisuudessa tulee kiinnittää entistä enemmän huomiota etäkäyttöratkaisujen tietoturvaan, etenkin silloin, kun etäkäyttöratkaisu suunnitellaan mobiililaitteita varten.

TAMPERE POLYTECHNIC
Degree Programme in Electrical Engineering
Automation Engineering
Paakkunainen, Kristian
Remote Control of Production Control Systems
Engineering Thesis
37 pages, 1 appendix
Thesis Supervisor
Mikko Numminen, MSc
Commissioning Company
Indel Automation Oy. Supervisor: Pasi Mattila
April 2005
Keywords
remote control, remote use, remote work, virtual private network, VPN

ABSTRACT

Travels in relation to the maintenance of automation systems causes unnecessary traveling expenses. That is why the remote use solution for remote control of production control systems has been developed during this engineering thesis. The remote use solution was based on virtual private network technology, remote control software and Siemens S7 Simatic Manager logic programming software. It was designed keeping data security in mind. The secure remote use solution was used to decrease unnecessary traveling expenses by reducing the need of travels in relation to the maintenance of automation systems. The developed remote use solution can be used as a basis for creating new remote use solutions. In the future, more attention has to be paid to data security. Especially, when developing a remote use solution for mobile devices.

SISÄLLYSLUETTELO

1 JOHDANTO

Tämän tutkintotyön aiheena on tuotannonohjausjärjestelmien etähallinta Internetin välityksellä. Aiheen taustalla on se, että tutkintotyön teettävä suunnittelutoimisto Indel Automation Oy on tähän asti joutunut aina lähettämään yhden työntekijöistään asiakkaan luo selvittämään vikaa ongelmatilanteessa. Tästä luonnollisesti aiheutuu kustannuksia sekä suunnittelutoimistolle että asiakkaalle. Matkoista asiakkaan luo syntyy tarpeettomia kustannuksia, etenkin, jos asiakkaan toimipiste sijaitsee hyvinkin kaukana, jopa toisessa maassa. On otettava huomioon myös se, että suunnittelutoimisto joutuu sitomaan ainakin yhden työntekijöistään vian selvittämiseen, jonka aikana hänen työpanostaan ei voida hyödyntää toisaalla. Etähallinta mahdollistaa sen, että automaatiojärjestelmien ylläpitoon käytettävän ajan ja etenkin matkustuksen tarve pienenee, jolloin sekä asiakas että suunnittelutoimisto säästävät ylläpidon kustannuksissa.

Tutkintotyön teettäjä on Indel Automation Oy, joka on alle 20 hengen täyden palvelun automaatioalan yritys. Sen toimipaikka sijaitsee Lahdessa. Yritys on erikoistunut eri teollisuuksien kone- ja tuotantoautomaatioon. Näitä ovat sahateollisuus, sellu- ja paperiteollisuus, elintarviketeollisuus, muoviteollisuus, pintakäsittelylaitokset, OEM-laitevalmistajat, metalliteollisuus ja sen jatkojalostus, konepajateollisuus sekä silta-automaatio. Indel Automation Oy kuuluu LSK-konserniin. Konserniin kuuluu myös LSK Electrics Oy, joka on harjoittanut teollisuuden sähköistämistä ja sähkölaitteiden tukku-, asennus- ja huoltotoimintaa jo yli 70 vuotta. LSK on lyhennetty sanoista Lahden Sähkö ja Kone.

Etähallinnan kohteena on Indel Automation Oy:n asiakas Stalatube Oy, jonka toimipaikka sijaitsee myöskin Lahdessa. Henkilökuntaa yrityksellä on noin 200 henkeä. Stalatube Oy on perheyritys, joka on erikoistunut valmistamaan kotikeittiöihin pesupöytiä, jätelajitteluvaunuja sekä liesikupuja. Tämän lisäksi yritys valmistaa postilaatikoita sekä erilaisia teräsputkipalkkeja.

Jatkossa käytetään tekstin selkeyttämiseksi Indel Automation Oy:stä nimeä Indel ja Stalatube Oy:stä nimeä Stala.

Tutkintotyössäni oli tehtävänä on muodostaa suojattu tietoturvallinen yhteys Indelin ja Stalan välille. Yhteys toteutetaan VPN-tekniikalla eli virtuaalisella yksityisverkolla. Tämän lisäksi tehtävänä on mahdollistaa Stalan tuotannonohjausjärjestelmien sekä tuotannonvalvontatietokoneen etähallinta ylläpidon kannalta. Indelin henkilökunnan tulee päästä VPN-yhteyden kautta käsiksi suoraan tuotannonohjausjärjestelmien logiikoihin. Se tapahtuu Internetin välityksellä suoraan Siemens S7 Simatic Manager -ohjelmistolla. Indelin henkilökunnan tulee lisäksi saada tuotannonohjausjärjestelmien tuotannonohjaustietokoneet (PC-paneelitietokoneet) sekä tuotannonvalvontatietokone (WinCC-tietokone) etähallintaan etähallintaohjelman avulla.

Tutkintotyöni tavoitteena on mahdollistaa automaatiojärjestelmien etäylläpito Internetin välityksellä. Tavoitteena on tehdä automaatiojärjestelmien ylläpidollisesta etähallinnasta mahdollisimman helppoa ja yksinkertaista unohtamatta tietoturvaa.

2 ETÄTYÖ

2.1 Etätyön määritelmä /1, s. 9./

Valtiovarainministeriön tutkimuksessa etätyö on määritelty seuraavasti: ”Etätyö on työtä, joka tehdään muualla kuin varsinaisella työpaikalla. Työ tehdään käyttäen etäkäyttöympäristöä.” Tutkimuksen mukaan etäkäyttöympäristöllä tarkoitetaan sitä paikkaa ja ympäristöä, jossa etäkäyttö tapahtuu. Etäkäytöllä taas tarkoitetaan tietotekniikkapalvelujen käyttöä varsinaisen työpaikkaverkon ulkopuolelta.

Jotta etäkäyttö olisi mahdollista, tarvitaan etäkäyttöratkaisu. Etäkäyttöratkaisu koostuu niistä laitteista ja ohjelmistoista, joilla etäkäyttö tehdään mahdolliseksi. Tässä tapauksessa etäkäyttöratkaisu koostuu VPN-yhteydestä, etähallintaohjelmasta, Siemens S7 Simatic Manager -ohjelmistosta ja niistä laitteista, joilla tuotannonohjausjärjestelmät sekä tuotannonvalvontatietokone on kytketty Internetiin.

Valtiovarainministeriön tutkimuksen mukaan etätyötä tehdään käyttäen etäkäyttöympäristöä, joka koostuu etäkäyttöratkaisusta. Etäkäyttöympäristönä on tässä tapauksessa esimerkiksi Indelin työntekijällä mukana oleva kannettava tietokone tai Indelin toimistossa sijaitseva tietokone.

2.2 Etätyön tarve

Etätyön lähtökohtana on syntynyt tarve tehdä töitä muualla kuin itse työkohteessa. Tarpeen syntymiseen vaikuttavat niin työstä aiheutuneet kustannukset, kuten työmatkakustannukset, kuin myös halu helpottaa päivittäistä työntekoa.

Tämän tutkintotyön myötä on haluttu tarjota asiakkaalle entistä nopeampaa ja edullisempaa automaatiojärjestelmien ylläpitoa. Tämä saavutetaan etähallinnalla, jolloin myös suunnittelutoimiston työntekijöiden työ helpottuu, kun työtä ei tarvitse välttämättä tehdä itse paikalla työkohteessa. Tästä syntyy siis säästöjä sekä asiakkaalle että suunnittelutoimistolle. Asiakas ei enää joudu maksamaan kalliista huoltokäynneistä. Vastaavasti suunnittelutoimisto ei joudu sitomaan työntekijää huoltokäyntiin pitkäksi aikaa, vaan huolto käy nopeasti verkon välityksellä. Tällöin huollon tehnyt työntekijä voidaan sitoa tekemään enemmän jotakin toista työtä huoltokäynteihin kuluneen ajan sijaan. Suunnittelutoimiston työntekijäkin hyötyy etätyöskentelystä, koska hänen ei tarvitse tehdä tarpeettomia työmatkoja asiakkaan luo.

Etätyön taloudellinen hyöty tulee esille etenkin silloin, kun asiakkaan työkohde on kaukana tai jopa ulkomailla. Tällöin esimerkiksi pienen tarkistuksen tekeminen tai logiikan ohjelmointivirheen korjaaminen tulee kohtuuttoman kalliiksi sekä asiakkaalle että suunnittelutoimistolle. Etätyön tarve on siis perusteltu.

2.3 Käytännön toteutus

Indelillä aiotaan hyödyntää etätyötä siten, että työntekijät voivat suorittaa automaatiojärjestelmien ylläpidon poistumatta suunnittelutoimistolta. Tässä vaiheessa ei ole tarkoitus laajentaa etätyön mahdollisuutta niin, että Indelin työntekijät voisivat työskennellä kotonaan, vaikka se olisikin teknisesti mahdollista. Tarkoituksena on siis säästää kustannuksissa vähentämällä tarpeettomien työmatkojen määrää.

Etätyö mahdollistetaan etätyöratkaisulla, joka on sidottu suunnittelutoimistoon. Etätyöratkaisussa Indelin tietokoneisiin asennetaan tarvittavat ohjelmat, jotta jokaisella tietokoneella olisi mahdollista tehdä ylläpidolliset toimenpiteet Internetin välityksellä. Vastaavasti Stalan tuotannonvalvonta- sekä tuotannonohjaustietokoneisiin asennetaan tarvittavat ohjelmat, joilla mahdollistetaan niiden etähallinta. Lisäksi automaatiojärjestelmien logiikoihin tehdään tarvittavat asetukset, jotta niihin saadaan etäyhteys logiikkaohjelmointiohjelmalla.

Fyysisiin laiteyhteyksiin ei tarvitse tehdä muutoksia, koska Indelin tietokoneet ja Stalan tuotannonohjaus- ja valvontatietokoneet sekä automaatiojärjestelmät ovat jo valmiiksi yhteydessä Internetiin. Indelin ja Stalan laitteet ovat palomuurilaitteiden takana. Stalan palomuurin asetuksiin on tehtävä muutoksia, jotta Indeliltä saadaan etäyhteys Stalan verkkoon. Muutokset palomuurin asetuksiin tekee Stalan verkkoa ylläpitävä IT-asiantuntija. Indelin palomuurin asetuksiin ei tarvitse tehdä muutoksia.

3 ETÄYHTEYDET

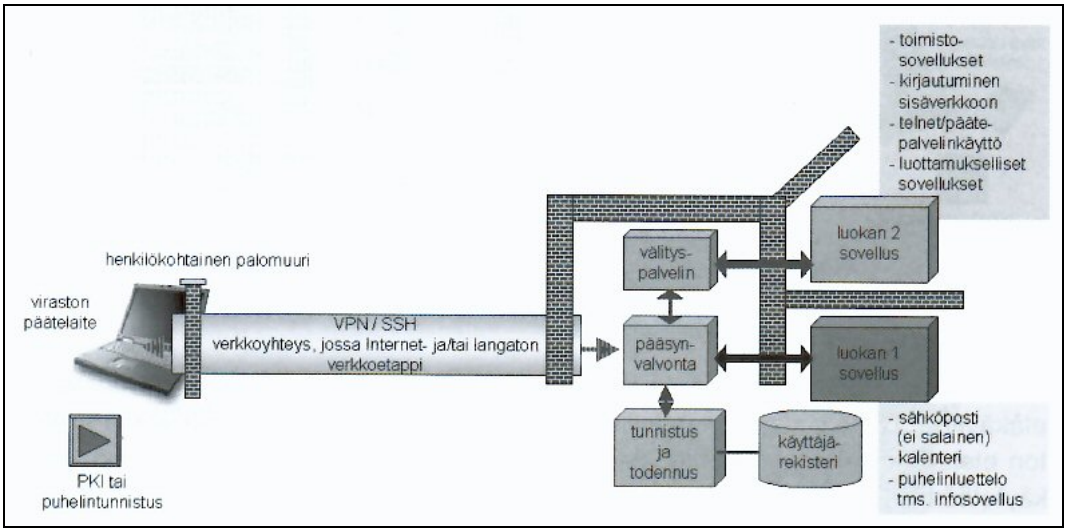
3.1 Yleistä

Etäyhteyksien luomisessa ei riitä pelkästään laitteiden kytkeminen toisiinsa ja yhteysasetusten määritteleminen. On otettava huomioon tiettyjä asioita ennen kuin voidaan luoda luotettava, helppokäyttöinen ja turvallinen etäyhteys. Näitä ovat

yhteystarpeet, laiteyhteyksien luominen, käytettävien ohjelmistojen valinta ja tietoturva.

Etäyhteyksien luominen lähtee siis liikkeelle yhteystarpeiden kartoituksesta, jota seuraa tarvittavien laite- ja tarvikehankintojen tekeminen laitteiden liittämiseksi Internetiin. Näiden kahden vaiheen jälkeen selvitetään, tarvitseeko yhteystarpeiden toteuttamiseksi hankkia jotakin ohjelmistoa, ja sitten hankitaan kyseinen ohjelmisto. Koko prosessin ajan on ensisijaisen tärkeää pitää mielessä tietoturva. Siksi onkin selvitettävä, mitä laitteilta tai ohjelmistolta vaaditaan riittävän tietoturvan takaamiseksi.

Valtiovarainministeriön tutkimuksen mukaan turvallisen etäkäytön luomiseksi on kolme vaihetta, kun käytetään turvattomia verkkoja. Nämä vaiheet ovat etäkäyttöpolitiikan määrittely, etäkäyttöpalvelujen luokittelu ja etäkäyttöluokkien hyväksyttävien etäkäyttöratkaisujen määritteleminen. Näiden vaiheiden jälkeen tutkimuksessa on päädytty muutamaan erilaiseen suositeltavaan etäkäyttöratkaisuun. Keskitytään niistä luokan 2 etäkäyttöratkaisuun, joka on lähes suunniteltua etäkäyttöratkaisua vastaava. Kuvassa 1 on esitetty minimivaatimukset siinä tapauksessa, että käytettävä verkkoyhteys kulkee Internetin kautta. Tutkimuksen mukaan päätelaitteen tulee olla viraston hallitsema eli tässä voidaan ajatella Indelin hallitsevan päätelaitteita. Lisäksi päätelaitteessa tulee olla henkilökohtainen palomuuri sekä VPN- tai SSH-valmiudet eli tarvittavat ohjelmat. /1, s. 65-66./



Kuva 1 Luokan 2 etäkäyttöratkaisu käytettäessä yleisiä verkkoyhteyksiä /1, s. 66/

Indelin ja Stalan välille suunniteltu etäkäyttöratkaisu vastaa perusperiaatteiltaan kuvan 1 etäkäyttöratkaisumallia lähes täysin. Päätelaitteita hallitsee Indel ja käytettävä yhteys on VPN-tyyppinen, jonka kumpaakin päätä suojaavat palomuurilaitteet. Koska käytettävät päätelaitteet ovat Indelin verkon sisällä, niin erillisiä henkilökohtaisia palomuuriohjelmistoja ei tarvitse asentaa jokaiseen päätelaitteeseen, koska Indelin verkon palomuurilaite suojaa yhteyden.

Etäyhteyden muodostuksessa ja etähallintaohjelmassa käyttäjätunnistus tulee tapahtumaan käyttäjätunnuksen ja salasanan avulla. Lisäksi etäyhteys on salattu eli yhteys on suojattu. Voidaan siis olettaa suunnitellun etäkäyttöratkaisun tietoturvan tason olevan riittävä.

3.2 Yhteystarpeiden määrittely

Tarkoituksena on muodostaa tietoturvallinen etäyhteys Indelin verkosta Stalan tehdasverkkoon. Näiden kahden yrityksen välille muodostetaan suojattu VPN-yhteys, jonka kautta liikennöidään sekä suoraan että etähallintaohjelman välityksellä. Indeliltä tulee saada yhteys jokaiseen Stalan tuotantolinjan logiikkaan suoraan Siemens Step 7 Simatic Manager -logiikkaohjelmointiohjelmistolla. Lisäksi tulee muodostaa yhteys tuotannonohjaus- sekä tuotannonvalvontatietokoneisiin etähallintaohjelman avulla.

Tuotantolinjojen logiikoita ohjelmointi sekä ohjelmien suorituksen tarkkailu tulee voida suorittaa Internetin välityksellä käyttäen logiikkaohjelmointiohjelmistoa. Tuotannonvalvonta- sekä tuotannonohjaustietokoneet tulee saada etähallintaan etähallintaohjelman avulla. Lisäksi niiden ja Indelin tietokoneiden välillä tulee voida siirtää tiedostoja.

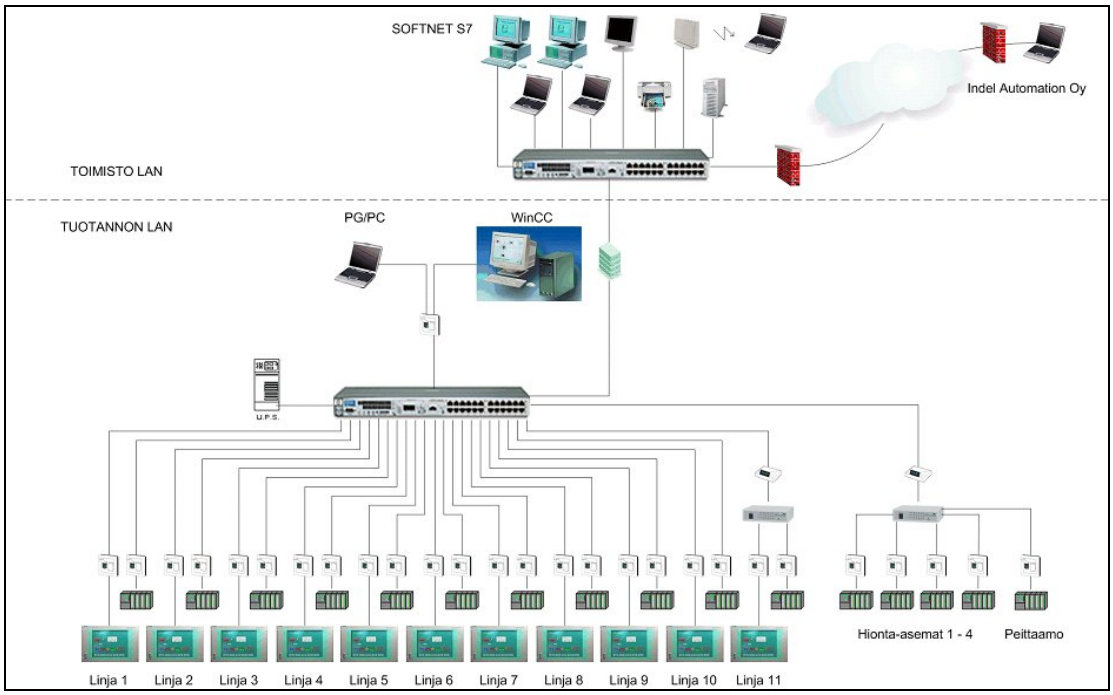
4 ETÄYHTEYKSIEN TOTEUTUS

4.1 Laiteyhteydet

Indelin verkko on normaali toimistokäyttöön suunniteltu yritysverkko. Indelin tietokoneet on kytketty Internetiin reitittimen kautta, joka on liitetty ADSL-modeemiin. Indelin verkkoa suojaa oma palomuurilaite, joka on kytketty reitittimen ja ADSL-modeemin väliin.

Stalan verkkoa suojaa myös oma palomuurilaite, jonka takana on toimistoverkon reititin. Tähän reitittimeen on kytketty kaikki Stalan toimistoverkon tietokoneet ja laitteet. Tämän lisäksi Stalalla on toinen toimistoverkosta erotettu tehdasverkko. Tätä kahden verkon erottamista toisistaan kutsutaan segmentoinniksi. Segmentoinnilla voidaan parantaa tietoverkon tietoturvaa rajoittamalla pääsyä tiettyihin verkon osiin. Tämän etäkäyttöratkaisun tapauksessa Indeliltä on estetty pääsy Stalan toimistoverkkoon. Indeliltä pääsee siis käsiksi vain Stalan tehdasverkkoon. Toimistoverkon reitittimen lisäksi Stalalla on erillinen tehdasverkon reititin, johon on kytketty kaikki tehdasverkon laitteet, kuten tuotannonohjaus- ja tuotannonvalvontatietokoneet sekä logiikat. Indeliltä muodostetaan yhteys suoraan tähän tehdasverkon reitittimeen, jolloin yhteys kulkee Stalan palomuurilaitteen ja toimistoverkon reitittimen kautta.

Kuvassa 2 on esitetty laiteyhteydet. Siinä näkyvät linjat ovat Stalan tuotantolinjoja ja niiden kohdalla olevat isot laatikot tarkoittavat tuotannonohjaustietokoneita. Tuotannonohjaustietokoneina käytetään kosketusnäyttöpaneeleja, jotka sisältävät keskusyksikön. Näppäimistönä käytetään erityistä tehdaskäyttöön tarkoitettua näppäimistöä, jossa on myös tappihiiri. Jokaisen linjan kohdalla näkyy myös pieni laatikko, joka tarkoittaa tuotantolinjan logiikkaa. Kuvassa näkyy lisäksi WinCC-tietokone, joka on tuotannonvalvontatietokone. Suurempi kuva laiteyhteyksistä löytyy liitteestä 1.



Kuva 2 Tiedonkeruuverkko /3/

4.2 VPN-yhteys

4.2.1 Johdatus virtuaalisen yksityisverkon käsitteeseen /2, s.7./

Ymmärtääksemme, mitä tarkoitetaan VPN-yhteydellä eli virtuaalisella yksityisverkolla (Virtual Private Network), on ensin tutustuttava hieman tietoverkkojen rakenteeseen. Bruce Perlmutter määrittelee tietoverkon (network) homogeeniseksi siirtojärjestelmäksi, jonka välityksellä systeemit voivat kommunikoida yksinkertaisia sääntöjä käyttämällä.

Perlmutterin mukaan verkkoja on erilaisia. Otetaan lähtökohdaksi kahden tietokoneen välinen verkko. Kun kaksi tietokonetta yhdistetään keskenään suoraan toisiinsa, syntyy tietoverkko. Syntynyttä tietoverkkoa kutsutaan lähiverkoksi eli Ethernet LANiksi (Local Area Network). Perlmutterin mukaan Ethernet LAN on verkko, joka yhdistää useita tietokoneita. Hänen mukaansa myös kaksi datapaketteja etäyhteyden välityksellä edestakaisin lähettävää reititintä muodostavat verkon. Tästä päästäänkin siihen ideaan, että ”Näitä samoja reitittimiä voidaan

käyttää yhdistämään kaksi Ethernet LANia käyttäen samaa kaukoyhteyttä.” Tällöin olemme päässeet lähemmäksi VPN:n käsitettä.

4.2.2 Virtuaalisen yksityisverkon määritelmä /2, s. 10-12./

Perlmutter määrittelee virtuaalisen yksityisverkon näin: ”***VPN*** *on tietoliikenneverkko, joka on rakennettu yrityksen yksityiseen käyttöön jaetun julkisen infrastruktuurin välityksellä. Tämä määritelmä kattaa kaksi ensisijaista sovellusta: etäyhteydet ja eri toimipaikkojen väliset yhteydet.*”. Hän olettaa suurimmaksi osaksi, että ”jaettu julkinen infrastruktuuri” on Internet, vaikka Internet on teknisesti ottaen osa siitä, mitä maailmanlaajuisesti on käytettävissä. Perlmutterin mukaan ratkaiseva kohta määritelmän kannalta on se, että Internet perustuu IP:hen (Internet Protocol). Perlmutterin mukaan IP:llä tarkoitetaan niitä tietoverkkostandardeja, joita yhdessä kutsutaan IP:ksi. VPN-ympäristössä tietoa käsitelläänkin juuri IP-sovellusvirtoina.

VPN:n toteutuksessa on kriittinen merkitys valtuuttamisella, todentamisella ja yksityisyydellä. Perlmutterin mukaan ne ovat itse asiassa tulleet keskeisiksi kysymyksiksi tämänhetkisessä tietoverkkoihin liittyvässä toiminnassa. Todennus ja salaus ovat kaksi tekniikkaa, joiden avulla lisätään ”yksityisyyttä” virtuaaliseen yritysverkottumiseen.

Yksi tärkeä todennuksen ja salauksen yhteydessä käytetty tekniikka on tunnelointi. Tunnelointi on yksinkertaisesti sanottuna yhtä protokollaa noudattavan datapaketin kapselointi toista protokollaa käyttävään datapakettiin, siis vastaava asia kuin kirjeen laittaminen kirjekuoreen. VPN:n kohdalla tämä kuori käsittää osoitteenmuodostuksen, salauksen, todennuksen ja pakkauksen eli siis VPN-palvelut, joita sovelletaan alkuperäiseen verkkopakettiin.

VPN:n yksityisyyttä eli käytännössä tietoturvaa käsitellään tarkemmin kohdassa 5, Tietoturva.

4.2.3 VPN-yhteyden toteutus

VPN-yhteys Indelin ja Stalan välille toteutettiin erillisellä ohjelmistolla. Ohjelmistoksi valittiin Check Point VPN-1, koska sitä käytettiin jo muihin tarkoituksiin Stalalla. Oli siis johdonmukaista käyttää kyseistä ohjelmistoa tämänkin yhteyden luomiseen.

Stalalle oli jo aikaisemmin asennettu Check Point VPN-1 SecuRemote -palvelinsovellus, joten Stalan päässä ei tarvinnut tehdä mitään määrittelyjä tai ohjelmistojen asennuksia. Sen sijaan Indelin testitietokoneelle asennettiin Check Point VPN-1 SecuClient -asiakassovellus. Testitietokoneena toimi tutkintotyön ohjaajan kannettava tietokone. Stalan IT-asiantuntija kävi Indelillä asentamassa testitietokoneeseen asiakassovelluksen. Tämän jälkeen muodostettiin VPN-yhteys Stalalle käynnistämällä asiakassovellus, johon kirjautumalla aukesi VPN-tunneli Stalalle. VPN-yhteyden toimivuus testattiin siten, että Internet-selaimeen syötettiin osoitteeksi Stalan 3-linjan IP-osoite muodossa ”\\xxx.xxx.xxx.xxx”. Tällöin päästiin käsiksi kyseisen tuotantolinjan tuotannonohjaustietokoneen hakemistorakenteeseen. VPN-yhteys havaittiin toimivaksi, joten yhteyden muodostus oli onnistunut.

4.3 Yhteydet logiikoihin

4.3.1 Yhteyksien muodostus

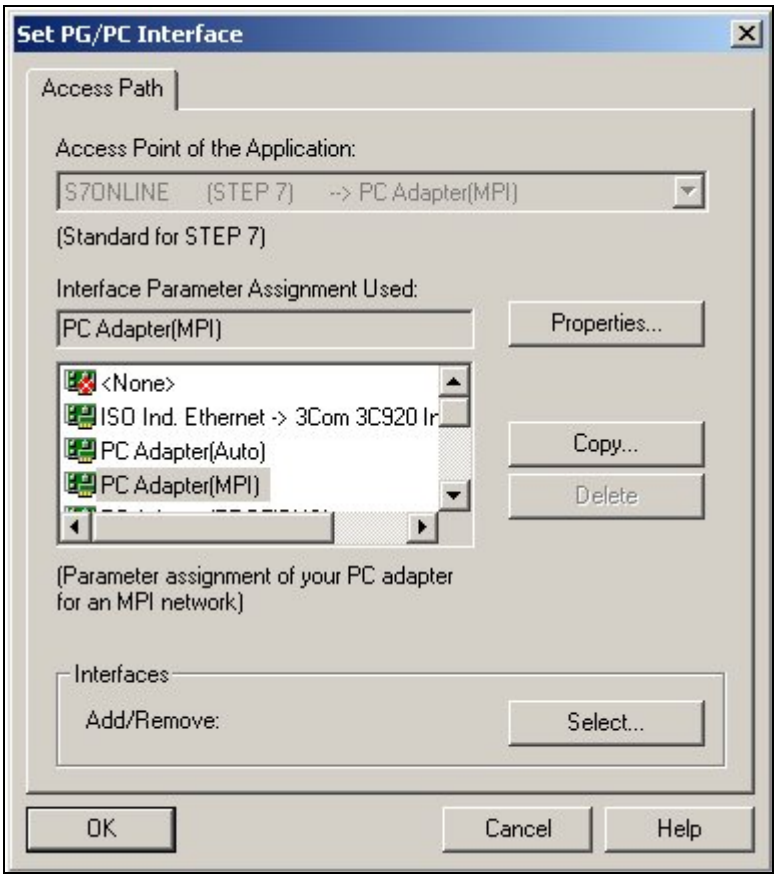
Stalan tuotantolinjojen automaatio on toteutettu Siemens S7 -logiikoilla, joita voidaan ohjelmoida Siemens S7 Simatic Manager -logiikkaohjelmointiohjelmalla. Yleensä ohjelmointilaite liitetään suoraan logiikkaan kaapelin välityksellä, jolloin logiikkaan saadaan yhteys logiikkaohjelmointiohjelman avulla. Tässä tapauksessa tarkoitus oli saada etäyhteys logiikoihin Internetin välityksellä, VPN-yhteystunnelin kautta, suoraan Simatic Manager -ohjelmalla. Ohjelmassa on tätä varten tuki IP-yhteydelle logiikkaan, kun logiikkaan on liitetty tarvittava verkkokortti.

Koska VPN-yhteys oli jo toiminnassa, päätettiin kokeilla yhteyttä logiikkaan *ping*-komennolla. Windowsin komentoriville syötettiin yhteyden testauskomento muodossa ”ping xxx.xxx.xxx.xxx”. Tällöin suoritettiin perustyypin kysely, jolla selvitettiin yhteyden toimivuus. Jos yhteys on kunnossa, tulostuu näytölle kyselyyn vastaukseen kulunut aika. Koska näytölle tulostui vain virheilmoitus ”tuntematon isäntä”, oli yhteyden muodostus epäonnistunut. Havaittiin, että jokaisen tuotantolinjan logiikan asetuksiin piti määritellä yhdyskäytävä (*Gateway*).

Yhdyskäytävän määrittely kertoo logiikalle reitin, jonka kautta se voi viestiä takaisin laitteelle, joka lähetti ensin sille viestin. Tässä tapauksessa yhdyskäytävänä käytettiin tehdasverkon reitittimen IP-osoitetta. Kun yhteyttä testattiin, niin ohjelmointilaitteen lähettämä viesti meni perille logiikkaan, mutta logiikka ei osannut lähettää viestiä takaisin ohjelmointilaitteelle. Tämä johtui siitä, että yhdyskäytävää ei ollut määritelty.

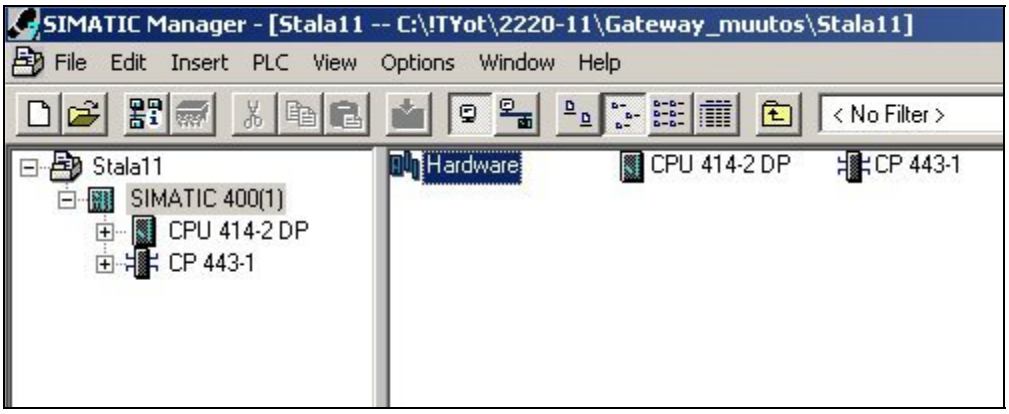
4.3.2 Yhdyskäytävien määrittely logiikoille

Yhdyskäytävät määriteltiin Siemensin S7-logiikoille laitteistokonfiguraation (*Hardware Configuration*) kautta. Tämä tehtiin siis käytännössä liittämällä kannettava tietokone logiikkaan MPI-väylän kautta. Tietokoneelta käynnistettiin logiikkaohjelmointiohjelma, johon määriteltiin ensin ohjelmointilaitteen ja logiikan välinen yhteystyyppi (*Set PG/PC Interface*). Yhteystyypiksi valittiin luettelosta MPI (kuva 3).



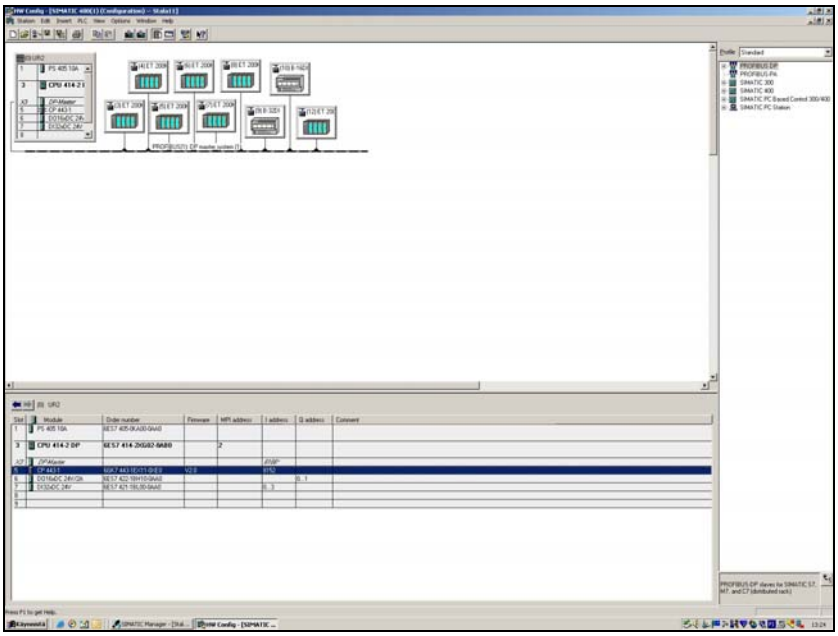
Kuva 3 Yhteystyypin valinta

Laitteistokonfiguraatioon päästiin käsiksi klikkaamalla auki laitteisto (*Hardware*) (kuva 4).



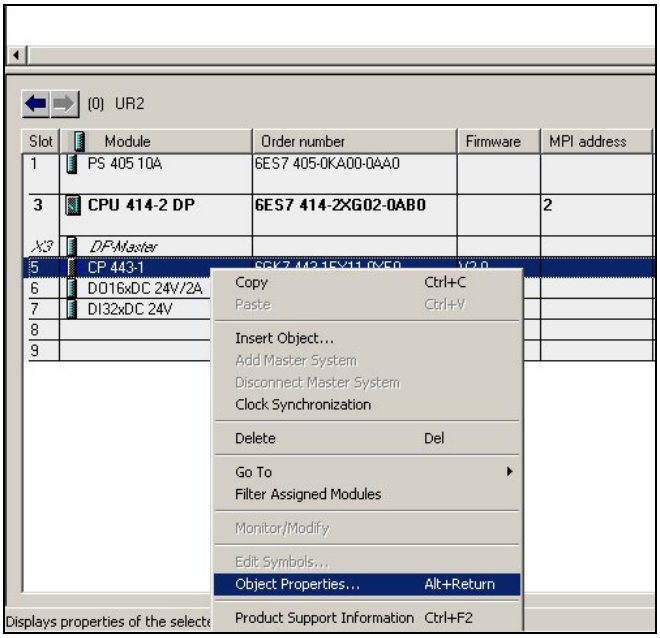
Kuva 4 Laitteisto

Tällöin aukesi kuvan 5 mukainen ikkuna, jonka kautta laitteistokonfiguraatio tehdään.



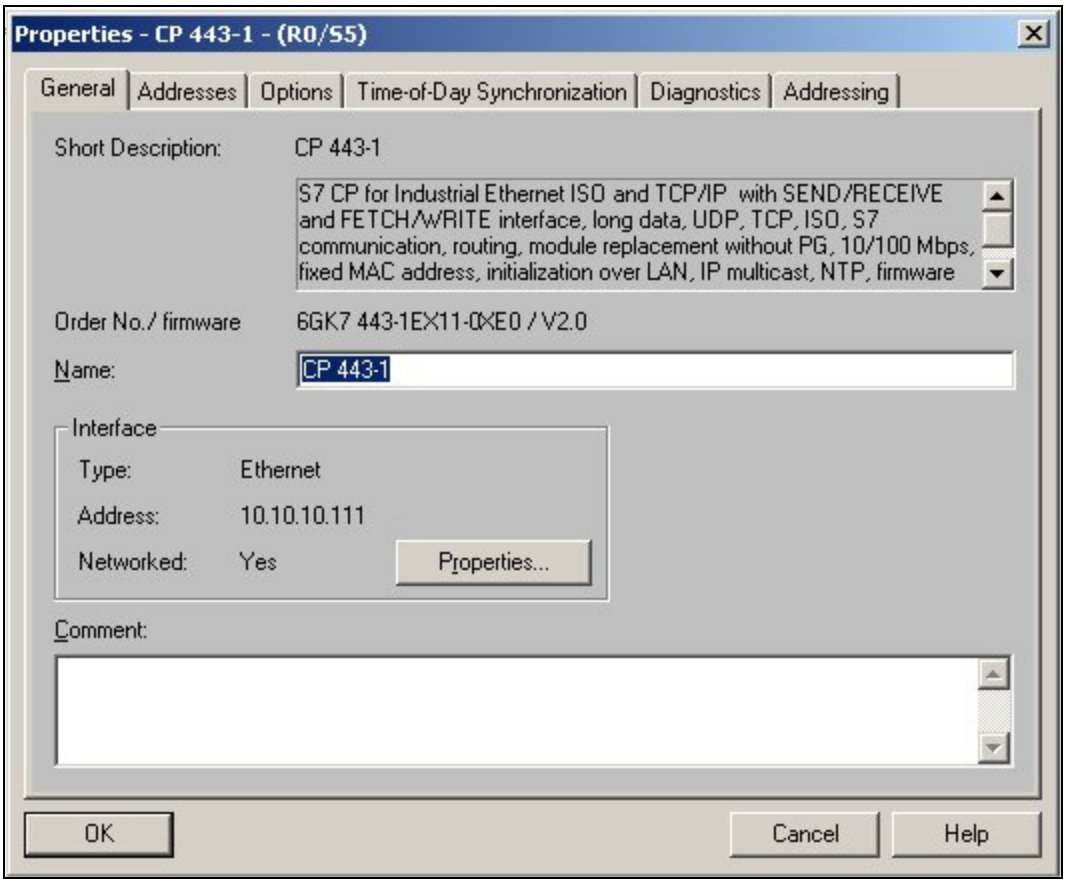
Kuva 5 Laitteistokonfiguraatio

Kuvan 5 laitteistokonfiguraatioikkunan alareunassa on lista logiikan laitteista (kuva 6). Klikkaamalla kommunikointiprosessoria (*CP*) hiiren oikealla näppäimellä saatiin auki luettelo, josta valittiin kohteen ominaisuudet (*Object Properties*).



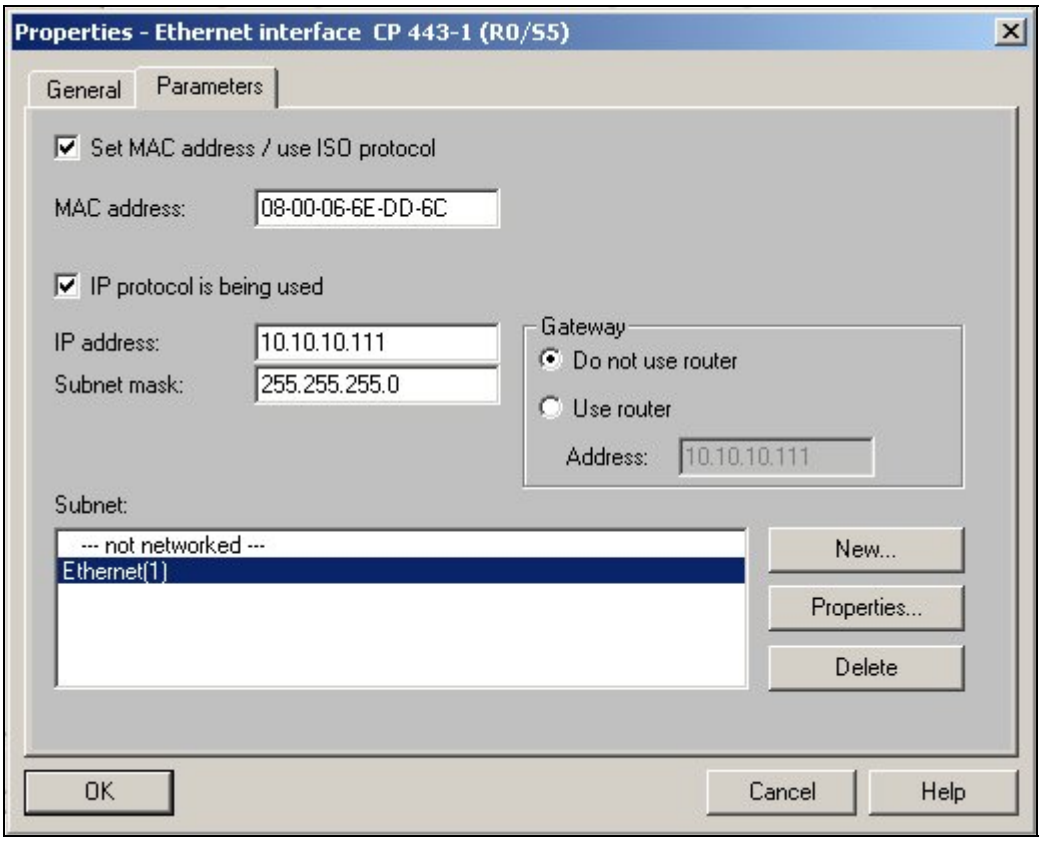
Kuva 6 Prosessorin ominaisuudet

Tällöin saatiin auki kuvan 7 mukainen ikkuna, josta löytyvät prosessorin ominaisuudet.



Kuva 7 Prosessorin ominaisuudet

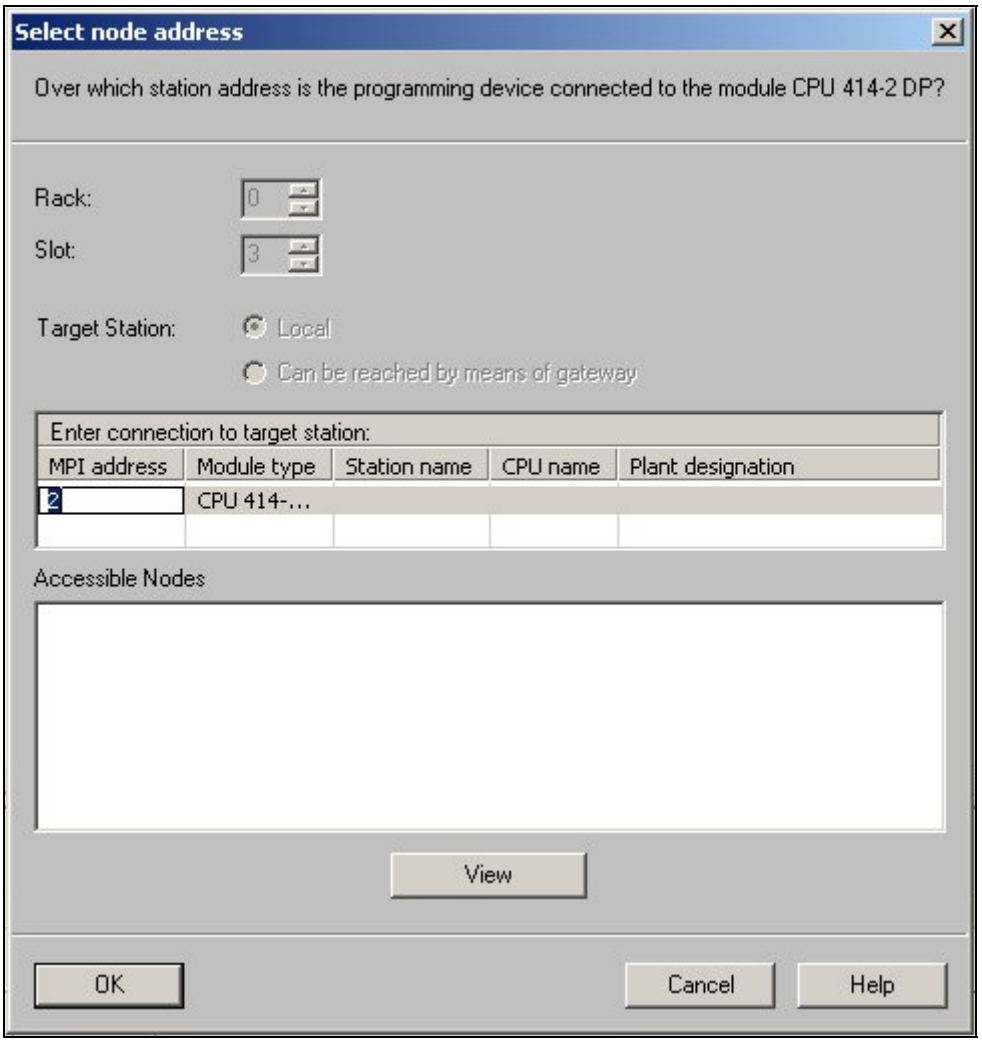
Ikkunasta valittiin liitynnän (*Interface*) ominaisuudet (*Properties*) yleisasetusten välilehdeltä (*General*), jolloin aukesi seuraava ikkuna (kuva 8).



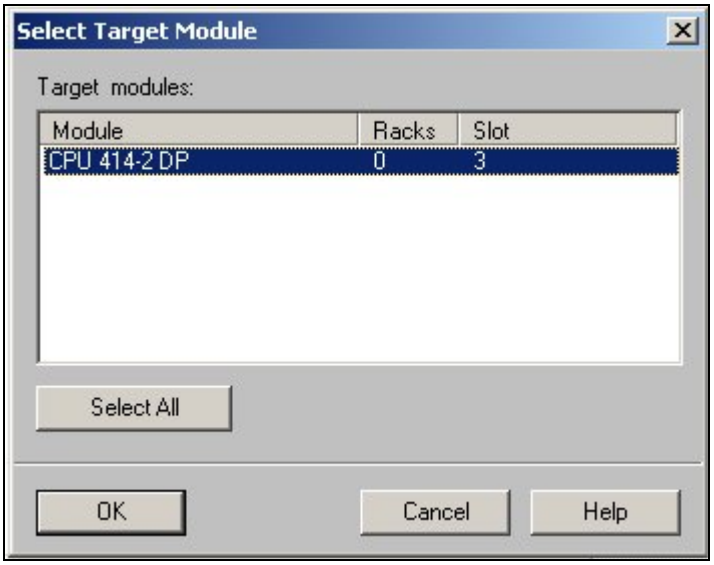
Kuva 8 Liitynnän ominaisuudet

Liitynnän ominaisuuksista löytyy yhdyskäytävän (*Gateway*) määrittely, josta klikattiin käyttöön reitittimen käyttö (*Use Router*). Reitittimelle annettiin osoitteeksi tehdasverkon reitittimen IP-osoite muodossa ”xxx.xxx.xxx.xxx”. Tällöin datapaketin vastaanottanut laite osaa lähettää vastauksen datapaketin lähettäneelle laitteelle ja yhteys logiikoihin saadaan muodostettua.

Kun muutokset logiikan asetuksiin oli tehty, tuli muutokset vielä ladata logiikkaan. Tämä tehtiin valitsemalla *PLC* → *Download to module*, jolloin aukesi seuraava ikkuna (kuva 9). Tässä ikkunassa määriteltiin se liityntäpiste (*Node*), johon haluttiin ottaa yhteyttä. Ohjelma tarjosi liityntäpisteen MPI-osoitteeksi arvoa 2, joka hyväksyttiin valitsemalla *OK*. Tällöin aukesi uusi ikkuna (kuva 10), josta valittiin kohdemoduuli (*Target Module*).



Kuva 9 Liityntäpisteen valinta



Kuva 10 Kohteena olevan moduulin valinta

Kuvan 10 ikkunasta valittiin siis kohdemoduuli (*Select Target Module*), johon muutokset haluttiin ladata. Tällöin aukesi ikkuna, jossa näytettiin latauksen edistyminen. Latauksen onnistuttua kohdemoduuli eli logiikka tuli vielä käynnistää uudelleen, jotta muutokset tulisivat voimaan. Tästä ohjelma antoi käyttäjälle kehotteen avaamalla uuden ikkunan, josta uudelleenkäynnistys hyväksyttiin valitsemalla *Yes*.

Näin oli määritelty yhdyskäytävä yhteen logiikkaan. Samat määrittelyt tuli tehdä jokaiseen logiikkaan, johon haluttiin ottaa yhteyttä logiikkaohjelmointiohjelmistolla. Näin menetellen kaikkien linjojen logiikoihin määritettiin yhdyskäytävät.

4.3.3 Yhteyksien uudelleentestaus

Yhteyksien toimivuutta testattiin aluksi *ping*-komennolla, johon kohteet vastasivat välittömästi. Seuraavaksi yhteyksiä testattiin logiikkaohjelmointiohjelmalla. Ohjelmointilaitteen ja logiikan väliseksi yhteystyypiksi (*Set PG/PC Interface*) valittiin TCP/IP. Tämän jälkeen avattiin 3-linjan projekti, jolloin otettiin yhteyttä 3-linjan logiikkaan. Yhteyden muodostus onnistui ja päästiin tarkkailemaan logiikkaohjelman suoritusta *Monitor*-toiminnalla.

Koska kaikki logiikat vastasivat *ping*-komennon kutsuun välittömästi ja logiikkaohjelmointiohjelmalla saatiin avattua tuotantolinjan logiikkaohjelma tarkkailtavaksi sekä muokattavaksi Internetin välityksellä, voitiin todeta yhteyksien muodostamisen onnistuneen.

5 TIETOTURVA

Tämän etäkäyttöratkaisun tietoturva riippuu täysin VPN-yhteyden tietoturvasta. VPN-tekniikassa käytetään tunnelointitekniikkaa, jolloin kaikki tietoliikenne Indelin ja Stalan välillä kulkee suojatun VPN-tunnelin kautta. Tällöin yritysten välistä verkkoa suojaamaan tarvitaan vain VPN-yhteyden tietoturva. Etähallinta-

ohjelman muodostaman etähallintayhteyden suojauksella ei siis ole merkitystä tietoturvan kannalta.

Check Point VPN-1 -ohjelmiston tietoturva perustuu tunnelointitekniikkaan. Perlmutterin mukaan tunnelointitekniikka toimii sillä periaatteella, että paketit tai kehykset kapseloidaan toisten pakettien tai kehysten sisään eli periaatteessa aivan kuin kirjekuori laitettaisiin toisen kirjekuoren sisään. Näin saadaan piilotettua yksityiset paketit ja niiden osoitteet julkisesti osoitettujen pakettien sisään. Tällä tavoin yksityisiä paketteja voidaan siirtää julkisen verkon eli esimerkiksi Internetin yli. /2, s. 106./

VPN-yhteyden tietoturvan takaamiseksi Check Point VPN-1 -ohjelmistossa on käytetty IPSec-tunnelointiprotokollaa. Tunnelointiprotokolla koostuu kolmesta perustekijästä: pakettitason todennuksesta, yhteyden salauksesta ja avaimenhallinnasta. Perlmutterin mukaan pakettitason todennus on toimenpide, jossa varmistetaan, että datan lähettäjät ovat todellisuudessa niitä, joita ne väittävät olevansa. Lisäksi todennuksella varmistetaan, että lähetetty data on yhtäläinen vastaanotetun datan kanssa. Salauksella tarkoitetaan toimenpidettä, jossa dataa sekoitetaan eli tavallaan lukitaan sellaiseen käsittämättömään muotoon, jonka pystyvät lukemaan vain ne, joilla on oikea avain hallussaan. Avaimenhallinta viittaa toimenpiteeseen, jossa sovitaan tai neuvotellaan salattu avainarvo lähettäjän ja vastaanottajan välillä. Nämä kolme perustekijää muodostavat IPSec-tunnelointiprotokollan ja tekevät siitä hyödyllisen VPN-protokollana. /2, s. 106-107./

VPN-yhteyden tietoturvasta puhuttaessa täytyy pitää mielessä myös käyttäjätodennus asiakaspäätteillä, jotta kuka tahansa ei pääse kirjautumaan ja käyttämään yhteyttä. Sama koskee myös etähallintaohjelmia. Siksi VPN-yhteyden asiakassovellukseen ja etähallintaohjelman asiakassovellukseen kirjautuminen on suojattu käyttäjätodennuksella. Vaikka VPN-yhteys olisi avattu kirjautumalla sen käyttäjäksi, on vielä erikseen kirjauduttava etähallintaohjelmaan. Etähallinnan käyttö on siis erittäin tarkkaan valvottua. Käyttäjätodennuksella varmistetaan sekä VPN-yhteyden että etähallinnan tietoturvallisuus käytön kannalta.

Tässä etäkäyttöratkaisussa hyödynnetty VPN-tekniikka on tietoturvatasoltaan käyttötarkoitukseen sopiva. VPN-tekniikalla toteutettu etäyhteys on suojattu sekä salauksella että käyttäjätodennuksella, joten etäyhteyttä ei pääse hyödyntämään kukaan ulkopuolinen. Tämän etäkäyttöratkaisun tietoturva on siis kunnossa.

6 ETÄHALLINTA

6.1 Yleistä

On tilanteita, jolloin olisi kätevää, jos ei tarvitsisi mennä itse paikalle kohteena olevan tietokoneen luo tekemään jotakin toimenpidettä. Tästä syystä on syntynyt idea tietokoneen etähallinnasta. Tietokoneen etähallinnalla tarkoitetaan sitä, että tietokonetta voidaan käyttää jonkin tietoverkon yli kuin istuisi itse tietokoneen ääressä. Etähallittava tietokone voi siis sijaita missä tahansa ja sitä voidaan hallita esimerkiksi Internetin välityksellä käyttäen jotakin toista tietokonetta etähallinnan apuvälineenä.

Etähallinnan toteuttamiseksi täytyy aina olla kaksi osapuolta eli käytännössä tietokonetta: palvelinkone ja asiakaskone. Palvelinkone on se tietokone, jota halutaan etähallita. Asiakaskone on se tietokone, jolla palvelintietokonetta etähallitaan. Jotta palvelinkonetta voitaisiin hallita asiakaskoneen avulla, täytyy siinä käyttää apuna erityistä etähallintaohjelmaa. Siksi useat eri valmistajat ovatkin kehittäneet oman näkemyksensä mukaisen etähallintaohjelman, jonka avulla tietokoneen etähallinta mahdollistetaan. Näkemyksellä viitataan yrityksen käsitykseen etähallinnasta.

Etähallintaohjelmissakin on aina kaksi osapuolta eli käytännössä sovellusta: palvelinsovellus ja asiakassovellus. Palvelinsovellus ”palvelee” asiakassovellusta toteuttamalla asiakassovelluksen lähettämät pyynnöt. Asiakassovelluksella voidaan muodostaa yhteys palvelinsovellukseen, mutta palvelinsovelluksella ei voida muodostaa yhteyttä asiakassovellukseen. Etähallinta on siis tällä tavoin yksisuuntaista.

Etähallintaohjelman avulla etähallittavalla tietokoneella voidaan tehdä lähes kaikki samat asiat kuin käytettäessä tietokonetta normaalisti itse paikalla koneen luona. Kuvitellaan tilanne, jossa jostain syystä menetettäisiin tietokoneen hallinta jollekin tuntemattomalle taholle. Tällöin etähallittava tietokone olisi täysin tämän tuntemattoman tahon hallinnassa ja tietokoneelta voitaisiin esimerkiksi poistaa kaikki tiedot kiintolevyltä. Jos tietokoneen sisältämä tieto on tärkeää, voi menetys olla todella suuri. Tästä syystä myös etähallintaohjelman tietoturvan tulee olla kunnossa ja siksi etähallintaohjelmaan pääsee kirjautumaan vasta kirjauduttuaan käyttämään suojattua VPN-yhteyttä. Koska etähallintaohjelma liikennöi suojatun VPN-yhteyden kautta, on etähallinta myös turvallista.

6.2 Etähallinnan tarpeiden määrittely

Yhteystarpeiden määrittelyn mukaan etähallinnan tarpeisiin luetaan tuotannonohjaus- ja tuotannonvalvontatietokoneiden etähallinta ja tiedostojen siirto Indelin ja Stalan välillä. Yhteystarpeiden määrittelyissä ei ole määritelty etähallinnan haluttuja ominaisuuksia tarkkaan, koska ainoa etähallinnalta vaadittu erityisominaisuus on tiedoston siirto. Etähallinnan tasoksi tiedostojen siirtomahdollisuuden lisäksi riittää siis se, että etähallittavan tietokoneen sovelluksia voidaan käyttää Internetin välityksellä.

6.3 Etähallintaohjelmien vertailu

Etähallintaohjelmien valmistajia on useita, ja jokainen valmistaja on luonut ohjelmiston oman näkemyksensä mukaiseksi. Etähallintaohjelmat eivät siten kaikki ole toimintaperiaatteiltaan samanlaisia. Perusperiaatteeltaan ne kuitenkin ovat samanlaisia siinä, että jokaisella ohjelmalla pystyy käyttämään tietokonetta Internetin välityksellä.

Etähallintaohjelman valintaprosessi aloitettiin kartoittamalla ensin vaihtoehdot. Aluksi etsittiin tietotekniikka-alan lehdistä ja Internetistä Suomessa saatavilla olevia etähallintaohjelmia. Vaihtoehtoja löytyi useita. Kaikki etähallintaohjelmat

olivat ulkomaisten yritysten valmistamia, mutta kahdella valmistajista on konttori Suomessa. Täysin kotimaista vaihtoehtoa ei löytynyt.

Etähallintaohjelmat voidaan jakaa karkeasti kahteen toimintaperiaatteeltaan eri tyyppiin. Ensimmäisen tyypin toiminta perustuu Internet-selainpohjaiseen käyttöliittymään. Siinä etähallinnan käyttöliittymänä toimii Internet-sivusto, johon kirjautumalla pääsee käyttämään etähallittavaa tietokonetta. Tämän tyypin etähallinnassa hyvä puoli on se, että etähallinnan asiakassovelluksen käyttöönotto ei vaadi kuin pienen sovellutuksen asennuksen selaimeen. Asiakassovelluksen käyttöönottoon riittää siis tietokone, jossa on Internet-yhteys. Etähallittavaan tietokoneeseen täytyy kuitenkin asentaa etähallinnan palvelinsovellus. Tämän tyyppisen etähallinnan käyttö ja käyttöönotto on todella yksinkertaista ja helppoa. Myös tietoturva on kunnossa käytettäisiin Internet-yhteyttä sitten mistä tahansa, koska Internet-sivustolle kirjauduttaessa siirrytään käyttämään suojattua SSH-yhteyttä (suojattu yhteyskäytäntö). Käyttäjätodennus sivustolle kirjauduttaessa tapahtuu käyttäjätunnuksen ja salasanan avulla. Tämän tyyppisessä etähallinnassa on kuitenkin pieni tietoturvariski. Jos käyttäjä on avannut etähallintayhteyden julkiselta koneelta ja poistuu koneensa luota hetkeksi, niin sillä aikaa joku voi käyttää yhteyttä. Tietoturvariski on siis olemassa vain käytettäessä julkisia tietokoneita asiakaspäätteinä. Julkisia tietokoneita ovat esimerkiksi kirjastojen ja Internet-kahviloiden tietokoneet.

Toisen tyypin etähallintaohjelmien toiminta perustuu siihen, että palvelinkoneelle asennetaan palvelinsovellus. Lisäksi jokaiseen asiakaspäätteeseen tulee asentaa asiakassovellus, jonka avulla etähallintayhteys muodostetaan. Tämän tyypin huono puoli on hidas käyttöönotto johtuen siitä, että asiakassovellus täytyy aina asentaa asiakaspäätteeseen ennen käyttöönottoa. Toinen huono puoli on se, että etähallintaa ei voi suorittaa miltä tahansa tietokoneelta, jossa on Internet-yhteys. Tämän tyypin etähallintaohjelman hyvä puoli on sen erittäin hyvä tietoturva. Etähallintayhteys muodostetaan kirjautumalla asiakassovellukseen, joka ottaa yhteyttä palvelinsovellukseen. Tämänkin tyypin etähallintaohjelmassa käyttäjätodennus tapahtuu käyttäjätunnuksen ja salasanan avulla.

Toisen tyypin etähallinnan tietoturvataso on parempi kuin ensimmäisen tyypin, mutta käyttöönotto ja käytettävyys on heikompaa kuin ensimmäisen tyypin etähallinnassa.

Suomessa saatavilla olevista etähallintaohjelmista valittiin viisi etähallintaohjelmaa vertailuun. Yhdellä näistä ohjelmista toteutettiin suunniteltu etäkäyttöratkaisu. Vaihtoehtoina olivat GoToMyPC, LapLink Gold 12, NetOp Remote Control 7.6, pcAnywhere 11.5 ja VNC. Näistä ohjelmista VNC (Virtual Network Computing) oli ainoa ilmainen vaihtoehto. Muiden ohjelmien hinnat vaihtelivat riippuen toimittajasta.

6.3.1 GoToMyPC /4/

Ensimmäisen tyypin etähallintaa edustaa ExpertCityn GoToMyPC. Kaikki muut ohjelmavaihtoehdot ovat toista tyyppiä. GoToMyPC toimii siten, että valmistajan Internet-sivustolta ladataan selaimen avulla pienikokoinen sovellutus, joka asentuu koneelle. Tämän jälkeen etähallintatoiminnot ovat käytettävissä kirjautumalla etähallittavalle tietokoneelle Internet-sivustolla. Kirjautuminen voidaan tehdä miltä tahansa Internetiin kytketyltä tietokoneelta.

Aluksi ExpertCity julkaisi kotikäyttäjille suunnatun version etähallintaohjelmasta, mutta pian sen jälkeen julkaistiin yrityskäyttöön suunnattu GoToMyPC Corporate -versio. Uusimmassa Corporate 4.0 -versiossa hyödynnetään kehittynyttä salausta.

GoToMyPC-ohjelmalla ei ole edustajaa Suomessa, vaan ohjelma on hankittavissa yrityksen Internet-sivustolta. Ohjelman hankinta ei itsessään maksa mitään, mutta ohjelman käyttö on maksullista. Ohjelman käyttö maksaa kuukaudessa 19,95 dollaria eli hieman yli 16 euroa. Ohjelman hinta koskee siis yhtä etähallittavaa tietokonetta, joten jokaisen tietokoneen lisenssistä joutuu maksamaan erikseen. Kahden tietokoneen lisenssi maksaa 29,95 dollaria kuukaudessa eli noin 24,50 euroa. Lisenssejä voi myös ostaa vuosilisensseinä, jolloin yhden koneen lisenssi tulee maksamaan kuukaudessa 14,95 dollaria eli hieman yli 12 euroa. Vastaavasti kahden tietokoneen vuosilisenssi tulee maksamaan kuukaudessa 22,45 dollaria eli

hieman alle 18,50 euroa. Pitkällä aikavälillä tämän tyypin etähallintapalvelun käyttö tulee kalliiksi.

Ohjelman hyviä puolia ovat sen helppokäyttöisyys ja yksinkertainen käyttöönotto. Huonoina puolina voidaan mainita pidemmällä aikavälillä hinta. Eräs huono puoli on myös se, että etähallinnan toteutuksessa käytetyn tekniikan vuoksi käyttäjien toimia ei voida valvoa tarkkaan.

6.3.2 LapLink Gold 12 /5/

LapLinkin LapLink Gold 12 edustaa toisen tyypin etähallintaa samoin kuin muutkin seuraavaksi esiteltävät etähallintaohjelmat. LapLink Gold -ohjelma toimii siten, että ohjelman asiakassovellus asennetaan asiakaspäätteelle ja etähallittavalle tietokoneelle asennetaan palvelinsovellus. Asiakassovellukseen kirjautumalla saadaan muodostettua etähallintayhteys etähallittavaan tietokoneeseen. Kaikki toisen tyypin etähallintaohjelmat toimivat tällä tavalla.

Laplink Gold tarjoaa oman käyttäjätodennuksen ja salauksen. Ohjelma voidaan sitoa käyttämään Windows-käyttöjärjestelmän käyttäjätodennusta, jolloin erillistä palveluun kirjautumista ei vaadita käyttäjältä. Ohjelmassa on sisäänrakennettu BitDefenderin virustorjunta, joka on toistaiseksi ilmainen, mutta muuttuu todennäköisesti jatkossa maksulliseksi palveluksi. Ohjelman asennus on helppoa ja onnistuu jopa push-asennuksena eli asiakassovelluksen asennus onnistuu myös verkon yli. Tällä tarkoitetaan sitä, että asiakassovelluksen asennus asiakaspäätteelle voidaan käynnistää ja suorittaa palvelinkoneelta käsin. Itse etähallintaohjelman käyttö on melko yksinkertaista ja helppoa.

LapLink Goldia myy Suomessa ainakin verkkokauppa Ohjelmistot.com. Kyseinen verkkokauppa ilmoittaa LapLink Gold 11.5 version hinnaksi 299 euroa per lisenssi. Version 12 hinta on ilmeisesti lähellä version 11.5 hintaa. Yksi lisenssi sisältää yhden tietokoneen etähallintaan tarvittavan ohjelman. Erillisiä asiakaslisenssejä ei ole, vaan lisenssi sisältää etähallintaohjelman lisäksi rajoittamattoman määrän asiakaslisenssejä. Tämän etähallintaohjelman käyttö tulee siis tällä laskutustavalla

kahden ensimmäisen käyttövuoden jälkeen edullisemmaksi kuin GoToMyPC:n käyttö. LapLink on tosin ilmoittanut, että ohjelman hyödyntämän etähallintapalvelun käyttö on toistaiseksi ilmaista, mutta muuttuu tulevaisuudessa maksulliseksi. Tällöin tämänkin etähallintaohjelman käyttö tulee kalliiksi, koska tulevaisuudessa sekä etähallintapalvelu että siihen integroitu virustorjunta ovat maksullisia palveluita, joista laskutetaan joko kuukausittain tai vuosittain.

LapLink Gold 12:n hyviä puolia ovat helppo ohjelmien asennus ja käytettävyys. Hyvä puoli on myös se, että ohjelma tukee useita erityyppisiä yhteysmuotoja, kuten USB:tä, lähiverkkoa, sarja- ja rinnakkaisliitäntää sekä modeemiyhteyttä. Ohjelman huono puoli on sen hinta tulevaisuudessa, kun etähallintapalvelu ja virustorjunta muuttuvat maksulliseksi.

6.3.3 NetOp Remote Control 7.6 /6/

Vertailun etähallintaohjelmista suorituskykyisin tiedonsiirrossa on Danware Datan NetOp Remoter Control 7.6. Danware Datalla on Turussa konttori, jonka toiminta perustuu täysin NetOp:n ympärille.

Stalan IT-asiantuntijan mukaan Stalalla on käytetty NetOp:tä 3D-grafiikan käsittelyyn Internetin välityksellä. Hänen mukaan NetOp oli ainoa testatuista etähallintaohjelmista, joka pystyi siihen. Muita testattuja etähallintaohjelmia olivat pcAnywhere ja VNC. Näiden muiden etähallintaohjelmien tiedonsiirto ei ole yhtä hyvin optimoitua kuin NetOp:ssa, joten niiden tiedonsiirron tehokkuus ei riittänyt 3D-grafiikan käsittelyyn Internetin välityksellä.

NetOp on yhteyden katkeamattomuuden kannalta vakaa etähallintaohjelma. NetOp on myös helppokäyttöinen ja joustava. Se tukee kaikkia yleisiä käyttöjärjestelmiä ja tietoliikenneprotokollia. Ohjelman tietoturvaominaisuudetkin ovat markkinoiden monipuolisimmat.

NetOp:n toiminta perustuu toisen tyypin etähallintaohjelmille tyypilliseen tyyliin asiakas- ja palvelinsovelluksien käyttöön. Ohjelman valmistaja on nimennyt

asiakassovelluksensa Guest-moduuliksi ja palvelinsovelluksen Host-moduuliksi. Valmistajan mukaan Guest-moduulilla varustetulla PC:llä voi etäkäyttää mitä tahansa tietokonetta, jossa on Host-moduuli. Vastaavasti Host-moduulilla varustettua tietokonetta voidaan etäkäyttää kaikilla tietokoneilla, joissa on Guest-moduuli.

NetOp Remote Control 7.6 -etähallintaohjelmaa myy Suomessa verkkokauppa Ohjelmistot.com. Verkkokauppa myy Guest- ja Host-lisenssiä 182 euron kappalehintaan. Yhden Guest-lisenssin ja yhden Host-lisenssin pakettihinta on 245 euroa. Tämän etähallintaohjelman käytölle ei ole lisenssin lisäksi muita maksuja, joten ohjelman käyttö on pidemmällä aikavälillä edullista. Koska Stalalla on jo käytössään joitakin kyseisen etähallintaohjelman lisenssejä, olisi lisälisenssien osto Stalan kontakteja käyttäen verkkokauppaa edullisempaa. Tällöin NetOp on pitkällä aikavälillä maksullisista etähallintaohjelmista edullisin vaihtoehto etäkäyttöratkaisun toteuttamiseksi.

NetOp:n hyviä puolia ovat sen suorituskyky, yhteyden vakaus, monipuolisuus, useiden käyttöalustojen ja tietoliikenneprotokollien tuki, erinomainen tietoturva sekä pitkällä aikavälillä edullisin hinta. Merkittäviä huonoja puolia tai puutteita ei tästä etähallintaohjelmasta löydy.

6.3.4 pcAnywhere 11.5 /7/

Maailman johtavaksi etähallintaohjelmaksi itseään mainostava Symantec pcAnywhere 11.5 on NetOp:n ja Laplinkin tyylinen etähallintaohjelma, jossa on myöskin asiakas- ja palvelinsovellus. Valmistaja on nimennyt asiakassovelluksen Remote-sovellukseksi ja palvelinsovelluksen Host-sovellukseksi.

pcAnywhere 11.5 on monipuolinen etähallintaohjelma, joka tukee useita eri käyttöjärjestelmiä. Ohjelma tarjoaa käyttäjälleen moninkertaisen suojauksen, jolla varmistetaan isäntätietokoneen ja etäistunnon turvallisuus. pcAnywhere tukee 13 erilaista käyttäjätodennustapaa, kuten esimerkiksi SecurID:tä. Ohjelmassa on myös ohjattu optimointitoiminto, jolla järjestelmän suorituskykyä voidaan parantaa.

Ohjelman kehittyneillä hakemisto- ja tiedostonsiirtotoiminnoilla tiedostojen etsiminen ja lataaminen on nopeaa ja helppoa.

Symantecilla on konttori Helsingissä ja pcAnywherea myy Suomessa esimerkiksi verkkokauppa Ohjelmistot.com. Verkkokauppa ilmoittaa yhden Host & Remote -lisenssin hinnaksi 379 euroa. Pelkkä Host-lisenssi maksaa 226 euroa. Kyseisen etäohjelman hankintahinta on kallis. Toki pitkällä aikavälillä ohjelman käyttö tulee edulliseksi, koska kertaluontoisen lisenssin lisäksi muita maksuja ei ole.

pcAnywheren ominaisuudet ovat monipuoliset, mutta ohjelma on selkeästi suunniteltu suurten yritysten etähallintaohjelmaksi. Ohjelmasta löytyy monipuolisia Help Desk -toimintoja ja -työkaluja, jotta etähallinnan ylläpito olisi helppoa.

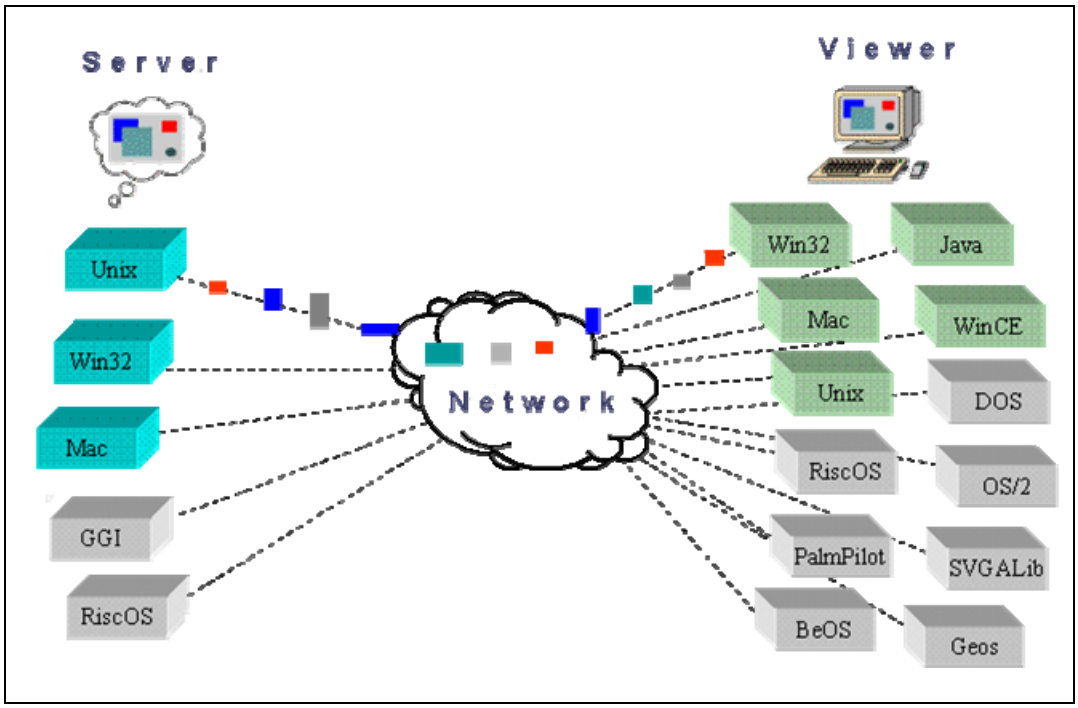
pcAnywhere 11.5:n hyviä puolia ovat sen monipuolisuus, apuohjelmat, työkalut, helppokäyttöisyys ja useiden käyttöjärjestelmien tuki. Huonoina puolina voidaan mainita korkea hankitahinta ja se, että ohjelmaa ei ole tarkoitettu pienten yritysten käyttöön.

6.3.5 VNC /8/

VNC (Virtual Network Computing) on avoimen lähdekoodin ilmaisohjelma. Avoin lähdekoodi tarkoittaa sitä, että kuka tahansa voi muokata ohjelman toimintaa ohjelmointiohjelmalla. Tällöin VNC:stä voi olla useita eri versioita, jotka ovat eri henkilöiden tekemiä. Alkuperäisen VNC-sovelluksen eli RealVNC:n on kehittänyt RealVNC Ltd. Muita tunnettuja ja paljon käytettyjä versioita alkuperäisestä RealVNC:stä ovat esimerkiksi TridiaVNC ja TightVNC. Kaikille VNC-ohjelmille on yhteistä se, että ne ovat ilmaisia ja pohjautuvat RealVNC:n lähdekoodiin.

VNC on etähallintaohjelma, joka sallii tarkkailla etähallittavaa tietokonetta eli palvelinta (Server) ja olla vuorovaikutuksessa sen kanssa. Tämä on toteutettu pienellä asiakasohjelmalla (Viewer), joka on asennettu toiseen, missä tahansa Internetissä olevaan tietokoneeseen. Näiden kahden tietokoneen ei edes tarvitse olla samaa tyyppiä. VNC:n kanssa voidaan käyttää useita erityyppisiä käyttö-

järjestelmiä ja asiakaspäätteitä. VNC:llä voi siis olla yhteydessä esimerkiksi Linux-koneeseen Windows-koneella. Etähallintaa voidaan toteuttaa joko käyttäen perinteistä tietokonetta tai kämmentietokonetta. Kuvassa 11 on esitetty asiakaspäätteen liittäminen etähallittavaan koneeseen Internetin välityksellä.



Kuva 11 Palvelin- ja asiakaslaitteen liittäminen toisiinsa VNC:n avulla

VNC:n muodostaman etähallintayhteyden tietoturva ei ole lainkaan hyväksyttävä yrityskäytössä, koska VNC käyttää vanhentunutta salaustekniikkaa. Tämä ei ole kuitenkaan este VNC:n käytölle tässä etäkäyttöratkaisussa, koska suunnitellun etäkäyttöratkaisun tietoturvan varmistamiseksi vain VPN-yhteyden täytyy olla suojattu. VNC:n täytyy sisältää vain käyttäjätodennus sen tietoturvan takaamiseksi.

VNC-ohjelmista keskitytään vain Constantin Kaplinskyn ylläpitämään projektiin nimeltä TightVNC. Syynä tähän on se, että TightVNC on ainoa ilmaisista VNC-ohjelmista, jonka ominaisuuksiin kuuluu tiedoston siirto. Koska tiedoston siirto on yksi yhteystarpeiden määrittelyiden mukaisista vaatimuksista, on TightVNC ainoa mahdollinen vaihtoehto VNC-ohjelmista.

TightVNC:n hyviä puolia ovat useiden käyttöjärjestelmien ja päätelaitteiden tuki, sekä ohjelman ilmaisuus. Huonoja puolia ja puutteita ohjelmassa on useita verrat-

tuna muihin esiteltyihin etähallintaohjelmiin. TightVNC on kuitenkin ominaisuuksiltaan riittävä tämän etäkäyttöratkaisun tarpeisiin.

6.4 Etähallintaohjelman valinta

Suunniteltuun etäkäyttöratkaisuun tarvittavan etähallintaohjelman valintakriteereinä olivat tiedoston siirto-ominaisuus ja mahdollisimman monipuoliset ominaisuudet mahdollisimman edulliseen hintaan. Koska kaikista etähallintaohjelmista löytyy vaadittu tiedoston siirto-ominaisuus, jää ainoaksi vaatimukseksi mahdollisimman monipuoliset etähallintaominaisuudet mahdollisimman edulliseen hintaan. Tästä syystä päädyttiin ilmaiseen TightVNC-ohjelmaan.

TightVNC sisältää tasoltaan riittävät tiedostonsiirto-ominaisuudet ja riittävän monipuoliset etähallintaominaisuudet suunnitellun etäkäyttöratkaisun toteuttamiseksi. Koska ohjelma on lisäksi ilmainen, oli järkevää valita TightVNC käytettäväksi etähallintaohjelmaksi.

Ohjelman voi ladata koneelleen ilmaiseksi Internetistä osoitteesta:
http://www.tightvnc.com.

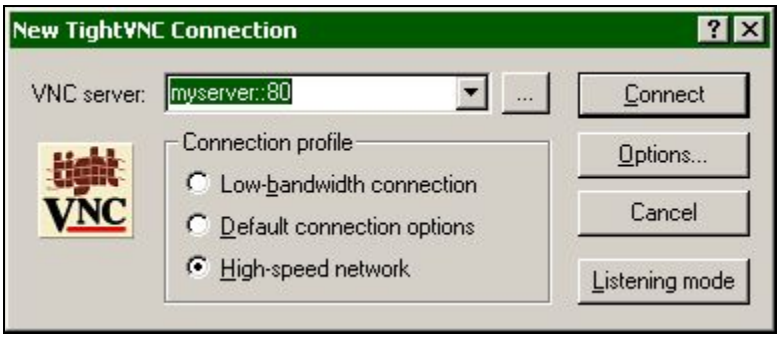
6.5 Etähallinnan toteutus /8/

Etähallinta toteutettiin käyttäen TightVNC-etähallintaohjelmaa. TightVNC on siis VNC-pohjainen etähallintaohjelma eli käytännössä alkuperäisen RealVNC-ohjelman paranneltu versio.

Aluksi asennettiin TightVNC-ohjelman palvelinsovellus eli TightVNC Server tuotannonohjaus- ja tuotannonvalvontatietokoneisiin. Palvelinsovelluksen asennusta varten tietokoneelle tuli kirjautua järjestelmänvalvojan tunnuksin, jotta asennus onnistuisi. Ohjelman asennuksen aikana asennusvaihtoehdoista valittiin sovelluksen rekisteröinti palveluksi (*Register as Service*) ja palvelun käynnistys ohjelman asennuksen päätyttyä (*Start Service After Finish*). Tällöin

palvelinsovellus suoritetaan Windows-käyttöjärjestelmän taustapalveluna aina, kun tietokone käynnistetään. Tällöin etähallittavaan tietokoneeseen saadaan yhteys, vaikka tietokoneelle ei olisi kirjauduttu käynnistyksen jälkeen. Asennuksen jälkeen aukesi ikkuna, johon määriteltiin palvelinsovelluksen salasana, jonka avulla siihen voitiin muodostaa etäyhteys. Salasanan määrityksen jälkeen asetusikkuna suljettiin ja tämän jälkeen ohjelma on toiminnassa taustapalveluna aina tietokoneen ollessa päällä.

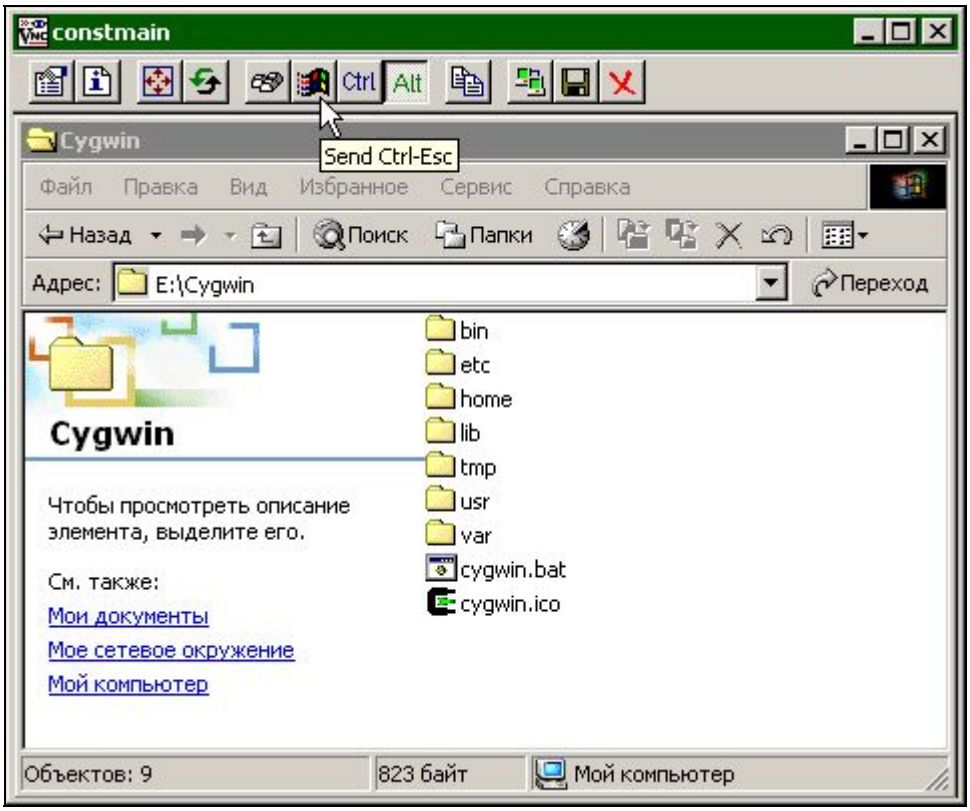
Seuraavaksi testitietokoneeseen asennettiin TightVNC-ohjelman asiakassovellus eli TightVNC Viewer. Asennuksen jälkeen ohjelma käynnistettiin, jolloin aukesi kuvan 12 näköinen ohjelmaikkuna.



Kuva 12 Uuden etähallintayhteyden luominen

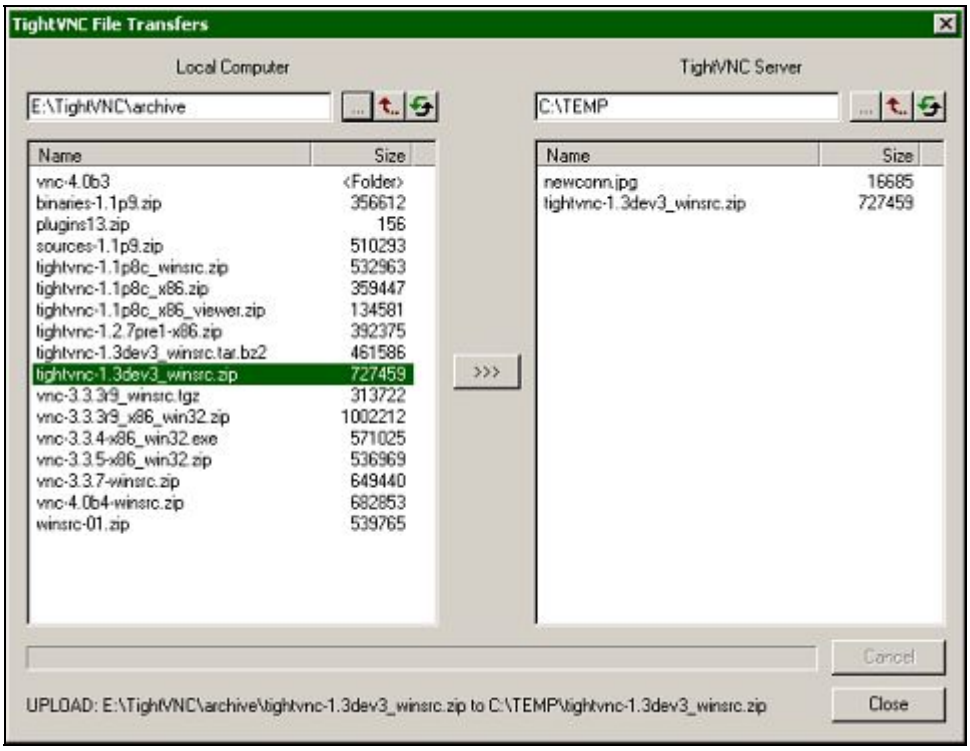
Ikkunaan syötettiin VNC-palvelimen (*VNC server*) osoite. Osoitteeksi syötettiin tuotannonohjaustietokoneen IP-osoite muodossa: ”\\xxx.xxx.xxx.xxx”. Tällöin yhteys muodostetaan suojatun VPN-yhteyden kautta, eikä suojaamattoman Internet-yhteyden kautta. Ikkunasta voitiin myös valita käytettävän yhteyden nopeus. Etähallintayhteyden avaaminen valitulla osoitteen muodolla edellytti, että VPN-yhteys oli päällä eli oli kirjauduttu VPN-asiakassovellukseen.

Etähallintayhteys avattiin klikkaamalla *Connect*. Tällöin aukesi uusi ikkuna, jossa etähallintaohjelma kysyi salasanaa. Tähän syötettiin nyt sama salasana, joka oli määritelty palvelinsovelluksen asetuksiin asennuksen yhteydessä. Syöttämällä oikea salasana saatiin avattua etähallintayhteys. Se näkyi tietokoneen näytöllä uutena, kuvan 13 näköisenä ikkunana.



Kuva 13 Etähallinnan yhteysikkuna

Ohjelmaikkunan sisällä on toinen ikkuna, jossa näkyy etähallittavan tietokoneen näyttö sellaisena kuin se näkyisi tehtaalla koneen luona. Tämän näytön kautta etähallittavaa tietokonetta voidaan käyttää samoin kuin olisi itse etähallittavan tietokoneen luona. Etähallintaohjelmasta voitiin avata erillinen ikkuna tiedoston siirtoa varten klikkaamalla ohjelmaikkunan ylävalikosta kuvaketta, jossa on kaksi nuolta. Tiedoston siirtoikkuna on kuvan 14 näköinen.



Kuva 14 Tiedoston siirtoikkuna

Tiedoston siirtoikkunassa näkyy vasemmalla listaus asiakaspäätteen tiedostoista ja oikealla listaus etähallittavan tietokoneen tiedostoista. Tiedoston siirto tapahtuu valitsemalla siirrettävät tiedostot ja klikkaamalla tämän jälkeen listausten välistä löytyvää nuolinappia. Nuolinapin nuolten suunta kertoo tiedoston siirron suunnan.

Tiedoston siirron toimintaa testattiin siirtämällä tiedosto Indeliltä Stalan tuotannonohjaustietokoneelle. Lisäksi ohjelman toimintaa ja suorituskykyä testattiin avaamalla tuotannonohjaustietokoneelta tuotantolinjan ohjausohjelma. Avatusta ohjelmasta katsottiin linjan käyntitietoja sekä muita tietoja. Etähallintayhteys toimi moitteettomasti, joten etähallintayhteys oli muodostettu onnistuneesti.

7 YHTEYKSIEN TESTAAMINEN

Yhteyksien testaaminen tehtiin avaamalla ensin VPN-yhteys Indelin ja Stalan välille kirjautumalla VPN-yhteyden asiakassovellukseen. Tämän jälkeen käynnistettiin TightVNC-ohjelma, jolla otettiin vuorollaan yhteyttä jokaiseen tuotannonohjaustietokoneeseen. Etähallintayhteyksien toimintaa testattiin tarkkailemalla

tuotannonohjaustietokoneiden ohjausohjelmien näyttöjä. Etähallintayhteydet toimivat normaalisti kaikkien muiden, paitsi yhden tuotantolinjan tapauksessa. Tämän yhden tuotantolinjan paneelitietokoneeseen ei saatu yhteyttä millään tapaa. Kyseinen tuotantolinja oli ilmeisesti sammutettu.

Etähallintayhteyksiä testattiin myöhemmin uudelleen. Tällöin avattiin taas VPN-yhteys ja käynnistettiin TightVNC-ohjelma, johon syötettiin yhteysosoitteeksi vuorollaan jokaisen testattavan tuotannonohjaus- ja tuotannonvalvontatietokoneen IP-osoite muodossa: ”\\xxx.xxx.xxx.xxx”. Jokaisen koneen toimintaa tarkkailtiin etähallintaohjelman kautta ja etähallintayhteydet havaittiin toimiviksi. Etähallinta-yhteydet oli muodostettu onnistuneesti.

Yhteyksiä tuotantolinjojen logiikoihin testattiin jo aikaisemmin siinä vaiheessa, kun kyseiset yhteydet luotiin. Silloin yhteydet kaikkien tuotantolinjojen logiikoihin toimivat normaalisti, eikä ole syytä olettaa tilanteen muuttuneen. Etäyhteyksiä logiikoihin testattiin kuitenkin vielä *ping*-komennolla. Jokaisen tuotantolinjan logiikan IP-osoitetta kutsuttiin syöttämällä Windowsin komentoriville *ping*-komento muodossa: ”ping xxx.xxx.xxx.xxx”. Jokaisen tuotantolinjan logiikan ip-osoitteesta tuli vastaus välittömästi, joten etäyhteydet logiikoihin oli muodostettu onnistuneesti.

Yhteyksien testaamisen lopputuloksena oli, että kaikki yhteydet toimivat suunni-tellulla tavalla.

8 TULEVAISUUDEN NÄKYMÄT

Etäyhteydet ja etähallinta saavat tulevaisuudessa yhä suuremman merkityksen, kun tekniikka kehittyy ja nopeat Internet-yhteydet yleistyvät. Tulevaisuutta ovat myös mobiililaitteet, kuten kannettavat tietokoneet, PDA-laitteet (kämmentietokoneet) sekä monikäyttöiset matkapuhelimet. Tulevaisuudessa etäyhteyksiä ja etähallintaa hyödynnetään näiden mobiililaitteiden kautta. Tällöin kiinteän työpisteen merkitys vähenee ja etätyön merkitys kasvaa. Etätyötä tullaan tulevaisuudessa tekemään yhä

enemmän nykyisten organisaatiomallien muuttuessa etätyöhön paremmin soveltuviksi. Tällöin tarvitaan kehittyneitä etäkäyttöratkaisuja, joilla etätyö mahdollistetaan. Etäkäyttöratkaisujen ohella kehittyvät myös niiden uhat, kuten esimerkiksi virukset, joten tulevaisuuden etäkäyttöratkaisujen tietoturvaa on myös kehitettävä.

Etätyössä on tulevaisuus, jonka monet organisaatiot ovat jo valinneet ja monet tulevat valitsemaan. Siksi etätyön toteuttamiseen tarvittavien organisaatiokohtaisten etäkäyttöratkaisujen kehitys on tärkeää.

LÄHTEET

Painetut lähteet

1 Turvallinen etäkäyttö turvattomista verkoista. Valtiovarainministeriö, Hallinnon kehittämisosasto 2003. 83 s.
2 Perlmutter, Bruce – Zarkower, Jonathan, VPN – Virtuaaliset yksityisverkot. Edita Oyj. Helsinki 2001. 269 s.

Sähköiset lähteet

3 Tiedonkeruuverkko. [Kuva]. Indel Automation Oy 2005.
4 GoToMyPC. [www-sivu]. [viitattu 20.3.2005] Saatavissa: http://www.gotomypc.com
5 LapLink. [www-sivu]. [viitattu 20.3.2005] Saatavissa: http://www.laplink.com
6 NetOp. [www-sivu]. [viitattu 20.3.2005] Saatavissa: http://www.netop.com
7 Symantec. [www-sivu]. [viitattu 20.3.2005] Saatavissa: http://www.symantec.com
8 TightVNC. [www-sivu]. [viitattu 20.3.2005] Saatavissa: http://www.tightvnc.com